US 20170195285A1

(19) **United States**

(12) **Patent Application Publication**

Kakhki et al.

(10) **Pub. No.: US 2017/0195285 A1**

(43) **Pub. Date: Jul. 6, 2017**

(54) **DETECTING AND MITIGATING REGISTRAR COLLUSION IN DROP-ADD ACQUISITIONS OF DOMAIN NAMES**

(71) Applicant: **VERISIGN, INC.**, Reston, VA (US)

(72) Inventors: **Arash Molavi Kakhki**, Boston, MA (US); **Andrew West**, Reston, VA (US); **Nipun Jawalkar**, Fribourg (CH); **Vincenzo Russo**, Belp (CH)

(21) Appl. No.: **14/985,569**

(22) Filed: **Dec. 31, 2015**

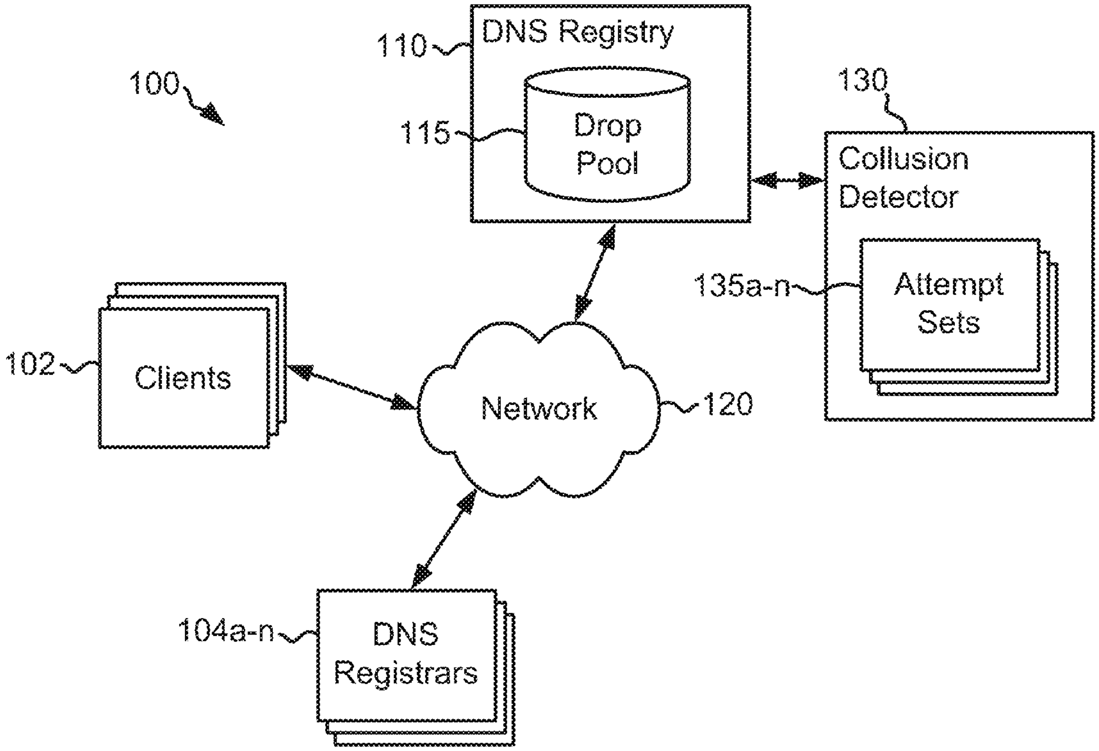
Publication Classification

(51) **Int. Cl.**
H04L 29/12 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 61/3005*** (2013.01); ***H04L 61/1511*** (2013.01); ***H04L 61/3025*** (2013.01)

(57) **ABSTRACT**

Systems and method for detecting domain name system (DNS) registrar collusion include a collusion detector at a registry. The collusion detector obtains information related to name acquisition requests submitted by DNS registrars attempting to acquire domain names in a drop pool of expired domain names and provides attempt sets containing the domain names targeted by the DNS registrars for acquisition. Each attempt set contains at least one targeted domain name that a respective DNS registrar attempted to acquire via at least one name acquisition request. The collusion detector determines a degree of similarity between two or more attempt sets corresponding to a pair of the DNS registrars, estimates a likelihood of collusion between the pair of DNS registrars based on the degree of similarity, and performs any mitigation action warranted by the likelihood of collusion.


100
110
DNS Registry
115
Drop Pool
130
Collusion Detector
135a-n
Attempt Sets
102
Clients
Network
120
104a-n
DNS Registrars